

REMARKS

The Office Action dated December 16, 2006, has been received and carefully considered. In this response, claims 17-22 and 27 have been canceled.

I. THE ALLOWANCE/ALLOWABILITY OF CLAIMS 1-16 AND 23-26

Applicant notes with appreciation the indication on page 2 of the Office Action that claims 1-16 and 23-26 are allowable.

II. THE PATENTABILITY REJECTION OF CLAIMS 17-22 AND 27

One page 2 of the Office Action, claims 17-22 and 27 were rejected as being directed to non-statutory subject matter. Although Applicant disagrees with this rejection, Application has nonetheless canceled claims 17-22 and 27.

In view of the above, Applicant respectfully requests that the above patentability rejection be withdrawn.

III. CONCLUSION

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number, in order to expedite resolution of any issues and to expedite passage of the

Patent Application
Attorney Docket No.: 57983.000033
Client Reference No.: 13424ROUS02U

Present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

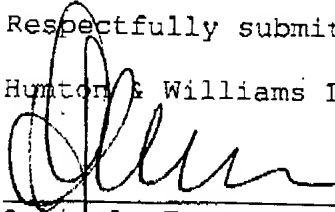
To the extent necessary, a petition for an extension of time under 37 CFR § 1.136 is hereby made.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0206, and please credit any excess fees to the same deposit account.

Respectfully submitted,

Hunton & Williams LLP

By:


Ozzie A. Farres
Registration No. 43,606

TEA/OAF/dja

Hunton & Williams LLP
1900 K Street, N.W.
Washington, D.C. 20006-1109
Telephone: (202) 955-1500
Facsimile: (202) 778-2201

Date: February 13, 2007

APPENDIX A

1 (Previously Presented). A method for preventing information losses due to network node failure, the method comprising the steps of:

operatively connecting at least one backup node to a primary node;

synchronizing the at least one backup node and the primary node;

receiving, from a first endpoint, ingress traffic in the primary node;

replicating the ingress traffic to the at least one backup node;

outputting, from the primary node, primary egress traffic;

outputting, from the at least one backup node, backup egress traffic;

determining if the primary node has failed;

transmitting, to a second endpoint, the primary egress traffic if it is determined that the primary node has not failed; and

transmitting, to the second endpoint, the backup egress traffic from a selected one of the at least one backup nodes if it is determined that the primary node has failed,

wherein the backup egress traffic from the selected one of the at least one backup nodes replaces the primary egress traffic to the second endpoint and the backup node becomes the primary node for subsequent traffic.

2 (Original). The method of claim 1, wherein the primary node and the at least one backup node are network routers.

3 (Original). The method of claim 1, wherein the primary node and the at least one backup node are security engines for receiving encrypted ingress traffic and outputting decrypted egress traffic.

4 (Original). The method of claim 1, wherein the step of synchronizing the at least one backup node and the primary node further comprises the steps of:

transmitting synchronization information from the primary node to the at least one backup node.

5 (Original). The method of claim 4, wherein the step of transmitting synchronization information from the primary node to the at least one backup node further comprises the steps of:

transmitting at least one checkpoint message from the primary node to the at least one backup node, wherein the at least one checkpoint message includes static information

relating to the primary node as well as any outstanding session context for the primary node.

6 (Previously Presented). The method of claim 5, further comprising the steps of:

receiving, from the at least one backup node, a checkpoint message acknowledgment for each of said at least one checkpoint messages;

determining whether each of the checkpoint message acknowledgments was received prior to a change in flow state;

transmitting a synchronization declaration from the primary node to the at least one backup node if it is determined that each of the checkpoint message acknowledgments was received prior to a change in flow state; and

transmitting at least one new checkpoint message from the primary node to the backup node if it is determined that each of the checkpoint packet acknowledgments was not received prior to a change in flow state.

7 (Original). The method of claim 4, further comprising the steps of:

periodically assessing synchronization maintenance between the primary node and the at least one backup node.

8 (Original). The method of claim 7, wherein the step of periodically assessing synchronization maintenance further comprises the step of:

transmitting at least a portion of internal state information from the primary node to the at least one backup node sufficient to permit replication of primary node traffic on the at least one backup node.

9 (Original). An apparatus for preventing information losses due to network node failure, the apparatus comprising:

a primary node;

at least one backup node operatively connected to the primary node;

synchronizing means operatively connected to the primary node and the backup node for synchronizing the at least one backup node and the primary node;

means for receiving ingress traffic in the primary node from a first endpoint;

means for replicating the ingress traffic to the at least one backup node;

means for outputting primary egress traffic from the primary node;

means for outputting backup egress traffic from the at least one backup node;

determining means operatively connected to the primary node and the at least one backup node for determining whether the primary node has failed;

means for transmitting the primary egress traffic from the primary node to a second endpoint if the determining means determine that the primary node has not failed; and

means for transmitting the backup egress traffic from a selected one of the at least one backup nodes to the second endpoint if the determining means determine that the primary node has failed.

10 (Original). The apparatus of claim 9, wherein the primary node and the at least one backup node are network routers.

11 (Original). The apparatus of claim 9, wherein the primary node and the at least one backup node are security engines for receiving encrypted ingress traffic and outputting decrypted egress traffic.

12 (Original). The apparatus of claim 9, wherein the synchronizing means further comprise:

means for transmitting synchronization information from the primary node to the at least one backup node.

13 (Original). The apparatus of claim 12, wherein the means for transmitting synchronization information further comprise:

means for transmitting at least one checkpoint message from the primary node to the at least one backup node, wherein the at least one checkpoint message includes static information relating to the primary node as well as any outstanding session context for the primary node.

14 (Previously Presented). The apparatus of claim 13, further comprising:

means for receiving in the primary node, from the at least one backup node, a checkpoint message acknowledgment for each of said at least one checkpoint message;

second determining means for determining whether each of the checkpoint message acknowledgments was received prior to a change in flow state;

means for transmitting a synchronization declaration from the primary node to the at least one backup node if it is determined that each of the checkpoint message acknowledgments was received prior to a change in flow state; and

means for transmitting at least one new checkpoint message from the primary node to the backup node if it is determined that each of the checkpoint message acknowledgments was not received prior to a change in flow state.

15 (Original). The apparatus of claim 12, further comprising:

means for periodically assessing synchronization maintenance between the primary node and the at least one backup node.

16. (Previously Presented) The apparatus of claim 15, wherein the means for periodically assessing synchronization maintenance further comprise:

means for transmitting at least a portion of an internal state of the primary node to the backup node sufficient to permit replication of primary node traffic on the at least one backup node.

17-22 (Canceled).

23 (Previously Presented). The method of claim 1 wherein the step of replicating the ingress traffic to the at least one backup node comprises simultaneously passing a copy of the ingress traffic to the at least one backup node.

24. (Previously Presented) The apparatus of claim 9 wherein the means for replicating the ingress traffic to the at least one backup node comprises means for simultaneously passing a copy of the ingress traffic to the at least one backup node.

Patent Application
Attorney Docket No.: 57983.000033
Client Reference No.:13424ROUS02U

25 (Previously Amended). The method of claim 1 wherein the ingress and egress traffic comprise session context information.

26 (Previously Amended). The apparatus of claim 9 wherein the ingress and egress traffic comprise session context information.

27 (Canceled).